# REAL QUADRATIC FIELDS IN WHICH EVERY NON-MAXIMAL ORDER HAS RELATIVE CLASS NUMBER GREATER THAN ONE

AMANDA FURNESS AND ADAM E. PARKER

Abstract. Cohn asks if for every real quadratic field $\mathbb{Q}(\sqrt{m})$ with discriminant $d$ there exists a non-maximal order corresponding to $f > 1$ such that the relative class number $H_d(f) = h(f^2d)/h(d)$ is one. We prove that when $m = 46$ (and in seven other cases) there is no such order.

## 1. Introduction

In his 1801 *Disquisitiones arithmeticae*, Gauss made advances in the theory of binary quadratic forms and brought forward questions in class theory that continue to be fruitful areas of research. Earlier, Lagrange had defined what it means for two binary quadratic forms to be equivalent, but then Gauss defined the composition of two forms and proved that the group of equivalence classes of binary quadratic forms with given discriminant was finite. Gauss only considered even discriminants, but this was quickly resolved. The order of this group is the class number $h(d)$ [4].

In order to answer a conjecture of Gauss, Dirichlet in [3] studied relative class numbers $H_d(f) = h(f^2d)/h(d)$, where $h(f^2d)$ is the number of primitive quadratic forms of discriminant $f^2d$. He proved that for certain $d$ there are an infinite $f$ such that $h(f^2d) = h(d)$ implying $H_d(f) = 1$. Cohn in [2, p. 219] states, "It is not known if such an $f$ exists for each $d$." In this note, we prove that this is not always the case. In particular, if $m = 46$, then there is no non-maximal order with $H_d(f) = 1$.

**Theorem 1.1.** *If $m = 46$, then the relative class number $H_d(f) \neq 1$ for all $f > 1$.*

Like Gauss, Dirichlet's study was in the language of quadratic forms. It wasn't until Dedekind introduced ideals that the conjectures of Gauss (and results of Dirichlet and others) were rephrased in terms of quadratic fields. For our purposes $m > 0$ is a square free integer, $\mathbb{Q}(\sqrt{m})$ the corresponding field, and $d$ its discriminant. Cohn in [2, pp. 201-204] gives the correspondence between quadratic forms and ideals in $\mathbb{Q}(\sqrt{m})$. We could then restate the question, asking if every quadratic field has a non-maximal order corresponding to $f > 1$ so that the relative class number is one. In general we follow the notation of [1], [2, pp. 216-217].

## 2. Results

Rather that directly compute the ratio $h(f^2d)/h(d)$ we will use the following theorem:

**Theorem 2.1.** [1][2, p. 217] *Let $m$ be a fixed, square-free, positive integer, and $d$ be the field discriminant of $\mathbb{Q}(\sqrt{m})$. Let $\varepsilon_m$ be the fundamental unit of $\mathbb{Q}(\sqrt{m})$ written in the form $\frac{x+y\sqrt{m}}{z}$ where $z = 2$ if $m \equiv 1 \ (mod\ 4)$ and $z = 1$ if $m \equiv 2, 3 \ (mod\ 4)$. Define $\psi(f) = f \prod_{q|f} \left(1 - \left(\frac{d}{q}\right)\frac{1}{q}\right)$ where $\left(\frac{d}{q}\right)$ is the Legendre symbol and $q$ is prime. Define $\phi(f)$ to be the smallest positive integer such that $(\varepsilon_m)^{\phi(f)} \in \mathcal{O}_f$, i.e. $(\varepsilon_m)^{\phi(f)} = \dfrac{a+b\sqrt{m}}{z}$ where $b \equiv 0 \ (mod\ f)$ and $z$ is as above. Then*

$$H_d(f) = \frac{\psi(f)}{\phi(f)}.$$

Please note that because we write $\varepsilon_m$ in the form where we divide by $z$, the "y coordinate" of the fundamental unit will always be an integer, and so it make sense to ask if $f$ divides $y$. Notice that if one is able to find a prime $f$ that divides $m$ but does not divide $y$ in this notation, then that $H_d(f)$ will equal 1. One one hand, since $f|m|d$ we know the Legendre symbol is 0, and hence $\psi(f) = f$. On the other, since $H_d(f)$ is an integer, $\phi(f) = 1$ or $f$. And since we chose $f$ not dividing the $y$, we know $(\varepsilon_m)^1 \notin \mathcal{O}_f$. So $\phi(f) = f$ and $H_d(f) = 1$.

In the case of $m = 46$ it is impossible to find such an $f$ since the the fundamental unit is $\varepsilon_{46} = 24335 + 3588\sqrt{46} = 5 \cdot 17 \cdot 157 + 2^2 \cdot 3 \cdot 13 \cdot 23\sqrt{2 \cdot 23}$. This is first quadratic field with a fundamental unit with the property that $m$ divides $y$, and so is a natural candidate to consider more carefully.

We will now prove Theorem 1.1.

*Proof.* We'll start by considering primes $f$ which don't divide 46. Since $m = 46 \equiv 2 \pmod 4$, the discriminant is $d = 4 \cdot 46 = 184$, and $z = 1$. Because $f$ is prime, $\psi(f) = f - \left(\frac{184}{f}\right) = f - \left(\frac{46}{f}\right)$ is even.

We also know that the fundamental unit $\varepsilon_{46} = 24335 + 3588\sqrt{46}$. This is the smallest solution to the Pell equation $x^2 - y^2 46 = 1$. If we write $\varepsilon_{46} = a_1 + b_1\sqrt{46}$, then other solutions are of the form $(a_n + b_n\sqrt{46}) = (a_1 + b_1\sqrt{46})^n$. These obey the recurrence relations

$$a_{n+1} = a_1 a_n + 46 b_1 b_n$$
$$b_{n+1} = a_1 b_n + b_1 a_n.$$

We can write this in matrix notation as

$$\begin{pmatrix} a_1 & 46b_1 \\ b_1 & a_1 \end{pmatrix} \begin{pmatrix} a_n \\ b_n \end{pmatrix} = \begin{pmatrix} a_{n+1} \\ b_{n+1} \end{pmatrix}$$

or

$$\begin{pmatrix} a_1 & 46b_1 \\ b_1 & a_1 \end{pmatrix}^n \begin{pmatrix} a_1 \\ b_1 \end{pmatrix} = \begin{pmatrix} a_{n+1} \\ b_{n+1} \end{pmatrix}$$

or

$$\begin{pmatrix} a_1 & 46b_1 \\ b_1 & a_1 \end{pmatrix}^{n-k} \begin{pmatrix} a_k \\ b_k \end{pmatrix} = \begin{pmatrix} a_n \\ b_n \end{pmatrix}. \tag{2.1}$$

It will be helpful to recognize that all powers of this matrix have determinant 1 (since $a_1^2 - 46b_1^2 = 1$) and have a nice "almost diagonal" form:

$$\begin{pmatrix} a_1 & 46b_1 \\ b_1 & a_1 \end{pmatrix}^t = \begin{pmatrix} \alpha & 46\beta \\ \beta & \alpha \end{pmatrix}$$

for some $\alpha, \beta$.

We start by examining $(\varepsilon_{46})^{\psi(f)}$. We know $\phi(f)$ - the minimum exponent such that $(\varepsilon_{46})^t \in \mathcal{O}_f$ - must divide $\psi(f)$ because $H_d(f) \in \mathbb{Z}$. Therefore, $(\varepsilon_{46})^{\psi(f)} \in \mathcal{O}_f$. Said differently, for

$$\begin{pmatrix} a_1 & 46b_1 \\ b_1 & a_1 \end{pmatrix}^{\psi(f)-1} \begin{pmatrix} a_1 \\ b_1 \end{pmatrix} = \begin{pmatrix} a_{\psi(f)} \\ b_{\psi(f)} \end{pmatrix},$$

we know $f | b_{\psi(f)}$. Our goal, then will be to show $f | b_n$ for some $n < \psi(f)$.

We look $\pmod f$. From [5, p. 59] we know that the solutions to $x^2 - 46y^2 = 1 \pmod f$ form a cyclic group of order $f - \left(\frac{46}{f}\right)$ which is our $\psi(f)$. Therefore,

$$\begin{pmatrix} a_1 & 46b_1 \\ b_1 & a_1 \end{pmatrix}^{\psi(f)} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \pmod f.$$

It turns out that $\left(\begin{smallmatrix} a_1 & 46b_1 \\ b_1 & a_1 \end{smallmatrix}\right)^{\psi(f)/2} \pmod f$ is diagonal. To see this, we write $\left(\begin{smallmatrix} a_1 & 46b_1 \\ b_1 & a_1 \end{smallmatrix}\right)^{\psi(f)/2} = \left(\begin{smallmatrix} \alpha & 46\beta \\ \beta & \alpha \end{smallmatrix}\right)$. Then

$$\begin{pmatrix} \alpha & 46\beta \\ \beta & \alpha \end{pmatrix} \begin{pmatrix} \alpha & 46\beta \\ \beta & \alpha \end{pmatrix} = \begin{pmatrix} \alpha^2 + 46\beta^2 & 2 \cdot 46\alpha\beta \\ 2\alpha\beta & \alpha^2 + 46\beta^2 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \pmod f$$

Since $f$ was chosen not to divide 46, either $f$ divides $\alpha$ or $\beta$. If $f | \alpha$, then $46\beta^2 \equiv 1 \pmod f$. But at the same time, this matrix should have determinant $\alpha^2 - 46\beta^2 = 1$, which means $-46\beta^2 \equiv 1 \pmod f$, which gives a contradiction. Therefore $f | \beta$ and we see that

$$\begin{pmatrix} a_1 & 46b_1 \\ b_1 & a_1 \end{pmatrix}^{\psi(f)/2} = \begin{pmatrix} \alpha & 0 \\ 0 & \alpha \end{pmatrix} \pmod f.$$

Setting $n = \psi(f) - 1$ and $k = \psi(f)/2$ in equation 2.1 above, we obtain the equation

$$\begin{pmatrix} a_1 & 46b_1 \\ b_1 & a_1 \end{pmatrix}^{\psi(f)/2} \begin{pmatrix} a_{\psi(f)/2} \\ b_{\psi(f)/2} \end{pmatrix} = \begin{pmatrix} a_{\psi(f)} \\ b_{\psi(f)} \end{pmatrix}.$$

Multiplying on the left by $\left(\begin{smallmatrix} a_1 & 46b_1 \\ b_1 & a_1 \end{smallmatrix}\right)^{\psi(f)/2}$ gives the following equations

$$\begin{pmatrix} a_1 & 46b_1 \\ b_1 & a_1 \end{pmatrix}^{\psi(f)} \begin{pmatrix} a_{\psi(f)/2} \\ b_{\psi(f)/2} \end{pmatrix} = \begin{pmatrix} a_1 & 46b_1 \\ b_1 & a_1 \end{pmatrix}^{\psi(f)/2} \begin{pmatrix} a_{\psi(f)} \\ b_{\psi(f)} \end{pmatrix}.$$

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} a_{\psi(f)/2} \\ b_{\psi(f)/2} \end{pmatrix} = \begin{pmatrix} a_{\psi(f)/2} \\ b_{\psi(f)/2} \end{pmatrix} = \begin{pmatrix} \alpha & 0 \\ 0 & \alpha \end{pmatrix} \begin{pmatrix} a_{\psi(f)} \\ b_{\psi(f)} \end{pmatrix} \pmod f.$$

Therefore $b_{\psi(f)/2} \equiv \alpha b_{\psi(f)} \pmod f$, and since we already know that $f | b_{\psi(f)}$ we know that $(\varepsilon_{46})^{\psi(f)/2} \in \mathcal{O}_f$. Therefore $H_d(f) \geq 2$.

A computation shows that when $m = 46$ that $H_d(23) = 23$ and $H_d(2) = 2$, because in both these cases, $\varepsilon_{46} \in \mathcal{O}_f$.

Therefore, for all primes $f$, $H_d(f) > 1$. And since if $f | g$ then $H_d(f) | H_d(g)$, this proves that $H_d(f) > 1$ for all $f > 1$.

□

One might ask how many other $\mathbb{Q}(\sqrt{m})$ satisfy that every non-maximal order gives a relative class number $> 1$. If there are other quadratic fields where $m$ divides the $y$ coordinate of $\varepsilon_m$, then the above proof would show that these fields never have a (non-maximal) relative class number of 1. Quadratic fields with this property were studied in [6] while researching powerful numbers. They tested all $\mathbb{Q}(\sqrt{m})$ with $m < 10^7$ and found only 8 fields such that $m$ divides $y$. They are $m = 46$, 430, 1817, 58254, 209991, 1752299, 3124318 and 4099215. Therefore, for all *other* $\mathbb{Q}(\sqrt{m})$ with $m$ square-free and $< 10^7$ one can find a prime $f$ that divides $m$ but not $y$, which would give $H_d(f) = 1$.

2.1. **Acknowledgments.** The authors would like to thank the 2009 REU at Mount Holyoke College, in particular Giuliana Davidoff, for bringing relative class numbers to our attention. We would also like to thank Jeffrey Lagarias for his comments that greatly improved several parts of this paper.

## References

[1] H. Cohn, *A numerical study of the relative class numbers of real quadratic integral domains.* Math. Comp. **16** (1962), 127–140.

[2] H. Cohn, *A second course in number theory.* John Wiley & Sons Inc., 1962.

[3] P.G. Lejeune Dirichlet, *Une propriété des formes quadratiques a déterminant positif.* J. Math. Pures Appl. - Série 2. **1** (1856), 76–79.

[4] D. Goldfeld, *Gauss's class number problem for imaginary quadratic fields.* Bull. Amer. Math. Soc. (N.S.) **13** (1985), 23–37.

[5] A. Menezes, *Elliptic curve public key cryptosystems.* The Kluwer International Series in Engineering and Computer Science **234**, Boston, 1993.

[6] A. J. Stephens and H.C. Williams, *Some computational results on a problem concerning powerful numbers.* Math. Comp. **50** (1988), 619–632.

Amanda Furness, Department of Mathematics,, Indiana University, Bloomington, IN 47405, USA
*E-mail address*: afurness@indiana.edu

Adam E. Parker, Department of Mathematics and Computer Science,, Wittenberg University, P.O. Box 720, Springfield, OH 45501, USA
*E-mail address*: aparker@wittenberg.edu
*URL*: http://userpages.wittenberg.edu/aparker